# Mise en place progressive d'une IGC au CNRS

**Jean-Luc Archimbaud CNRS/UREC [jla]**

Cet article décrit la mise en place progressive d'une IGC [IGC], Infrastructure de Gestion de Clés, pour délivrer des certificats [certificats] au CNRS. Ce projet a eu plusieurs phases, avec une démarche "pas à pas". Sont présentés dans cet article :

- Les besoins du CNRS extrapolables pour tous les organismes géographiquement dispersés et ouverts de part leur activité ; et comment nous pensons que les certificats pourront répondre à ces besoins,
- La mise en place d'une autorité de certification CNRS-Test de février 2000 à avril juin 2001 : les choix d'architecture, les procédures, les utilisations et le bilan,
- La présentation de l'architecture choisie, de la politique de certification et des procédures de l'IGC CNRS,
- Quelques éléments sur la phase pilote avec certains sites, démarrée en mai 2001,
- Les choix à faire avant le déploiement à toutes les unités CNRS,
- Quelques mises au point concernant les certificats.

## 1. Les besoins

Le CNRS est un organisme de recherche fondamentale public. De part ses missions, il se doit de diffuser largement les connaissances scientifiques et il a de très nombreuses collaborations tant au niveau national qu'international. Il doit donc être ouvert. Mais cela ne veut pas dire que tout est public au CNRS et qu'il ne faut rien contrôler. Pour prendre un seul exemple, la partie gestion de son système d'information doit fonctionner avec les mêmes règles strictes que les autres administrations et que les entreprises.
Le CNRS comme les universités, dispose d'un bon réseau de communication. Quasiment tTous les laboratoires disposent d'un réseau local, sont connectés à Renater et à l'Internet avec des débits souvent meilleurs que les entreprises et les autres administrations, et quasiment tout le personnel possède une adresse électronique et utilise le réseau quotidiennement. On pourrait donc penser que la dématérialisation, c'est à dire l'utilisation des réseaux et des documents électroniques en remplacement du courrier postal et du papier, de tous les actes administratifs ou de toutes les procédures qui demandent des contrôles serait chose aisée. Il n'en est rien. Outre le besoin d'ouverture dans le travail de recherche fondamentale, le problème vient de la taille, de l'éclatement géographique et de la complexité de l'organisme. Pour donner quelques ordres de grandeur, la recherche se fait dans environ 1300 laboratoires, la plupart associés (aux universités, ...), dispersés sur l'ensemble du territoire (et même à l'étranger). Le CNRS compte 26 000 agents mais environ 80 000 personnes travaillent dans les laboratoires. La partie administration de l'organisme est elle-même éclatée sur 20 délégations régionales. Le système d'information comporte trois sous-ensembles presque indépendants qui sont l'informatique dans les laboratoires, les centres serveurs nationaux et l'informatique de gestion. Tout ceci utilise pour communiquer Renater, réseau ouvert, sans vraiment de contrôle d'accès. Ces conditions rendent très difficiles, voire impossible, la délimitation d'une zone interne, où l'on pourrait se sentir en confiance, c'est à dire la notion d'Intranet comme on le verra un peu plus loin.

Donnons maintenant quelques exemples concrets de besoin.

- Comme chacun sait, il n'y a pas d'authentification ni de garantie d'intégrité dans la messagerie électronique que nous utilisons. Ainsi toute la diffusion des notes officielles et toute communication de personne à personne avec un besoin de signature se fait sous forme papier par le courrier postal.
- Il n'y a pas non plus de confidentialité : ainsi toutes les procédures pour les élections, les notations, la gestion du personnel, la gestion financière, … utilisent encore le courrier postal.
- De nombreuses applications de gestion co-existent au CNRS, chacune nécessitant une gestion de comptes utilisateurs et de mots de passe. Outre le travail d'administration système engendré, cet état de fait met à mal la sécurité basée sur les mots de passe, certains personnels administratifs ayant de nombreux mots de passe à se souvenir pour accéder à plusieurs applications, ils utilisent les méthodes de mémorisation "les plus simples", telles que le post-it.





• De part la situation géographique des laboratoires, il est impossible de créer un Intranet CNRS ou pour un sous-ensemble du CNRS basé sur des réseaux physiques ou logiques (adresses IP). Ainsi il n'y a pas de serveur Web CNRS avec des informations réservées aux agents CNRS ou à des sous-groupes (départements scientifiques, groupes thématiques, ...). On pourrait essayer de faire la liste des numéros IP des laboratoires mais cette compilation fastidieuse ne serait pas assez précise : certains laboratoires peuvent utiliser un sous-réseau d'une entité non CNRS, des adresses dynamiques, certaines petits unités très excentrées utilisent les fournisseurs d'accès publics à l'Internet, les campus ont des systèmes de translationtraduction d'adresses, ... Donc l'adresse IP n'est pas une méthode fiable à 100 % d'authentification des machines.

• L'organisme achète certains logiciels avec une licence organisme. N'ayant pas d'Intranet, il est très difficile de diffuser ces logiciels de façon tout à fait contrôlée, uniquement aux unités CNRS. Il faut une gestion de liste de numéros IP, de mots de passe, ...

• De nombreuses revues scientifiques sont maintenant en ligne avec un accès contrôlé payant. Pour respecter les clauses des contrats d'accès à ces revues et plus généralement aux bases de données, là aussi faute d'avoir une manière simple (l'adresse IP par exemple) pour identifier toutes les "stations CNRS", il faut recourir à une gestion de compte avec mot de passe.

• Sur un autre registre, un problème perdure depuis longtemps : la transmission du mot de passe en clair sur le réseau lors de connexion à distance. Ainsi de nombreux chercheurs en mission à l'extérieur et qui se sont connectés sur une machine de leur laboratoire ont eu leur mot de passe découvert par des pirates qui avaient installé des logiciels d'écoute. Ces mots de passe ont ensuite été utilisés pour accéder de manière illicite aux machines du laboratoire.

• Une fonction de sécurité apparaît maintenant comme une priorité dans les projets de grilles de calcul et de données [Datagrid] qui visent à construire une toile planétaire regroupant des capacités de calcul, de mémoire, de stockage, de visualisation de données, ... : ces projets nécessitent une authentification de tous les acteurs, utilisateurs et ressources.

On pourrait trouver une solution sur mesure à chacun des besoins ci-dessus. Mais chacune ne résoudrait qu'un seul problème tout en étant grosse consommatrice de ressources humaines pour la mise en place et l'administration. Une autre stratégie est essayer d'avoir une fondation commune qui va permettre de combler toutes ces lacunes. Ce sont les certificats et les applications qui vont avec.

Car les certificats n'apportent absolument rien sans les standards et les applications qui peuvent les utiliser. Or ceux-ci sont maintenant nombreux, en voici quelques uns :

• S/MIME [S/MIME] est un standard messagerie qui permet authentification, intégrité (signature) et confidentialité (chiffrement) dans l'échange de messages électroniques. Il est supporté de base par Netscape et Internet Explorer (Outlook). Il n'est malheureusement pas supporté par Eudora.

• HTTPS [HTTPS] et SSL [SSL] sont des standards permettant des communications Web avec authentification du serveur et du client, intégrité et confidentialité des échanges. Il est aussi, de base, intégré dans Netscape et Internet Explorer.

• IPSec [IPSec] est un ensemble de standards qui permettent des communications sécurisées entre équipements réseau (routeurs ou stations IP). Intégré dans de nombreux routeurs, il utilise les certificats.

• IMAPS et POPS permettent d'accéder à ses boites aux lettres de manière sécurisée en utilisant l'authentification par certificat. Ils peuvent aussi être utilisés par Netscape et Internet Explorer.

D'autres applications que nous n'avons pas testées comme Stelnet et SFTP semblent permettre d'utiliser les certificats comme méthode d'authentification pour l'accès interactif et le transfert de ficher. La prochaine version du logiciel très répandu SSH [SSH] devrait permettre d'utiliser les certificats comme méthode d'authentification.

Lorsqu'une infrastructure de gestion de clés sera totalement déployée au CNRS, chaque personnel disposera d'un certificat qui contiendra des informations d'identification (nom, prénom, laboratoire, ...). Associé à cette infrastructure sera parallèlement en place tout un système d'annuaires LDAP permettant de retrouver le numéro d'agent d'une personne, sa fonction, son département scientifique, sa branche d'activité professionnelle, sa délégation, … Dans cette configuration, si l'on reprend la liste des besoins cités précédemment :

• La diffusion des notes officielles pourra se faire par messagerie électronique au standard S/MIME. Les messages seront signées électroniquement par l'émetteur (le Directeur Général, un Délégué, …). Le récepteur pourra vérifier automatiquement l'origine du message et son intégrité.

• Les votes, notations, … qui demandent la fonction de confidentialité, pourront aussi se faire par messagerie électronique S/MIME avec la fonction de chiffrement.

• Toutes les applications de gestion pourront baser leurs contrôles d'accès sur les certificats. Les utilisateurs n'auront plus qu'un seul mot de passe à connaître, celui permettant localement d'utiliser leur clé privée, les services informatiques n'auront plus à gérer des mots de passe utilisateur. Les applications contrôleront le certificat des utilisateurs et avec les informations complémentaires contenues dans les annuaires, en déduiront les droits d'accès de ces utilisateurs.

• On pourra créer des Intranet « logiques » dans les laboratoires, les délégations, au niveau de l'organisme … Il suffira de contrôler l'accès aux pages Web, non pas sur le numéro IP de la station de l'utilisateur, mais sur son certificat en utilisant HTTPS et SSL. On pourra par exemple choisir d'ouvrir un ensemble de pages à tous les utilisateurs qui possèdent un certificat CNRS, ces pages seront en fait l'Intranet CNRS général. De très nombreuses autres combinaisons de contrôles d'accès seront possibles avec les informations contenues dans les certificats et les annuaires associés. On pourra par exemple autoriser l'accès à des pages uniquement aux directeurs de laboratoires d'un département scientifique. Il suffira que chaque directeur ait un certificat et que l'on dispose d'un annuaire avec la fonction et le département de chaque personne.

• On pourra faire les mêmes types de contrôles mais pour accéder à des logiciels avec une licence organisme ou ministère ou à des bases de données électroniques payantes.

• L'utilisation de certificats pourra aussi éviter de transporter en clair sur le réseau les mots de passe lors d'accès à distance, en utilisant SSL dans IMAPS, POPS, Stelnet, SFTP et la prochaine version de SSH.

• Enfin pour les applications avec des ressources totalement distribuées, chaque élément pourra posséder un certificat (utilisateur, machine, disque, …) et tous les contrôles d'accès pourront reposer sur cette carte d'identité.

Tout ceci ne se mettra pas en place sans efforts. Il faudra effectuer certains développements logiciels, peut-être acheter des logiciels, mettre en place de nouvelles procédures, changer les anciennes, prendre de nouvelles habitudes, … Cela prendra du temps avant de se généraliser.

Mais si l'on dispose déjà d'une base solide de certificats, toutes ces applications pourront progressivement se développer ou migrer en s'appuyant sur ces éléments de confiance. De plus, l'informatique et les réseaux évoluant à la vitesse que l'on sait, de nouvelles applications vont rapidement arriver qui intégreront en standard les certificats.

Preuve que ce n'est pas une vision trop utopique, la législation est déjà prête dans ce domaine. En effet, une loi qui accepte la signature électronique comme une preuve au même titre que la signature manuelle a déjà été votée et le décret d'application est sorti [Décret signature électronique].

## 2. L'autorité de certification CNRS-Test

L'autorité de certification CNRS-Test [CNRS-Test] a été créée en février 2000, comme une plate-forme de tests. Le but était d'acquérir un savoir-faire sur les logiciels nécessaires dans une IGC, le travail engendré par les procédures, l'état des produits et les utilisations possibles des certificats. Malgré l'aspect tests, on désirait se mettre dans des conditions de production. Pour ce faire nous avons écrit un guide utilisateur en ligne et suivi une procédure de vérification de l'identité des personnes demandeuses de certificats.

Le nom CNRS-Test n'était pas anodin. Le but était de bien montrer que l'on était en phase de tests pour que la confiance dans ces certificats ne soit pas "trop importante". Nous voulions éviter aussi que ces certificats ne soient pas confondus avec les certificats délivrés pour l'autorité de certification CNRS qui serait mise en place plus tard. Il y a bien une limite de validité pour les certificats, un an dans le cas de CNRS-Test, mais ce sont néanmoins des objets qui, une fois créés, "vivent leur vie", sans que l'on puisse vraiment les détruire.

Les autorités de certification, d'enregistrement et le service de publication étaient une même personne, un ingénieur de l'UREC, et tous les logiciels de l'IGC étaient sur un seul serveur. Le certificat de l'autorité de certification CNRS-Test était auto-signé. Les produits utilisés pour l'IGC étaient OpenSSL [OpenSSL] et OpenCA [OpenCA] avec des adaptations. Par simplicité, la clé secrète de la CA était sur un CD, stocké dans un lieu protégé et accessible avec un mot de passe solide. La clé privée de chaque utilisateur demandeur de certificat était générée par l'utilisateur sur son poste et n'était ni connue, ni stockée par l'UREC.

Lorsqu'un utilisateur voulait un certificat CNRS-Test, il suivait un mode d'emploi disponible en ligne. Il téléphonait à l'administrateur de l'IGC qui faisait office d'autorité d'enregistrement. Celui ci prenait le nom de la personne et son numéro de téléphone. Puis il coupait la communication téléphonique. Après avoir vérifié que cette personne avait bien le numéro de téléphone donné (dans Labintel la base de données des personnels CNRS, certains annuaires en ligne, ...), l'administrateur rappelait la personne au téléphone. Au téléphone l'administrateur convenait avec le demandeur d'un mot de passe. Muni de ce mot de passe, l'utilisateur avec Netscape ou Internet Explorer accédait à un formulaire en ligne sur le serveur IGC. Il entrait ses coordonnées et toutes les informations nécessaires contenues dans le certificat. Sur le serveur IGC, l'administrateur montait le CD qui contenait la clé privée de l'autorité de certification CNRS-Test. Ce formulaire rempli, un couple de clés était généré sur le poste utilisateur, le serveur IGC récupérait la clé publique, générait le certificat et transmettait le certificat au navigateur de l'utilisateur qui l'installait. Des fonctions de Netscape ou d'Internet





Explorer, activées à distance par un serveur, permettent toutes ces opérations, sans logiciel supplémentaire sur le poste de l'utilisateur. Sur le serveur, l'accès au formulaire était alors fermé et le CD démonté. Pour terminer, un test d'échange de message signé et chiffré entre l'utilisateur et l'administrateur était fait pour vérifier que le certificat était correct.

Plus d'une centaine de certificats ont été délivrés avec cette procédure. Cette plate-forme de tests a ainsi permis de faire ressortir certains points qui ont servi ensuite pour définir une nouvelle architecture d'IGC et de nouvelles procédures. En voici quelques uns :

• Si l'on ne veut pas imposer une rencontre physique entre l'autorité d'enregistrement et l'utilisateur (où ce dernier présenterait ses papiers d'identité, ...), c'est à dire si l'on veut travailler à travers le réseau, l'autorité d'enregistrement doit bien connaître les personnes auxquelles il va autoriser la délivrance de certificats. Dans les faits, et c'était le but, cette autorité CNRS-Test a délivré des certificats a des personnes que l'UREC connaissait, donc la vérification d'un point central, l'UREC, suffisait. Mais pour l'ensemble du CNRS par exemple, on ne mettra pas une seule autorité d'enregistrement; on décentralisera et multipliera cette fonction.

• Les logiciels Netscape et Internet Explorer, dans les versions récentes, comportent toutes les fonctions nécessaires pour générer des couples de clés, envoyer la clé publique, récupérer un certificat, ... On n'a donc pas besoin de logiciel supplémentaire sur les postes clients pour ces fonctions.

• Le travail d'une autorité d'enregistrement de ce type a été d'environ une demi-heure par utilisateur. Vu le nombre de certificats à délivrer, il faut impérativement simplifier cette procédure et bien penser la partie organisationnelle de l'IGC. Il faut aussi former les utilisateurs, perdus dans les menus Nescape ou IE pas très clairs et trop bavards mais aussi qui n'ont pas compris les principes : qu'est-ce qu'un certificat ? qu'est-ce qu'une clé privée ? ...

• Un certificat contient l'adresse électronique de l'utilisateur. Pour que ce certificat puisse être utilisable, elle-ci doit correspondre exactement au champ “From” des messages émis par l'utilisateur. Or nombreux sont les utilisateurs qui ne savent pas que lorsqu'ils envoient un message, le serveur de messagerie du laboratoire ou du campus ajoute ou modifie leur adresse *(@iresco.fr devient @iresco.iresco.fr, @polycnrs-gre.fr* devient *@belledonne.polycnrs-gre.fr, ...)*. Il faut donc ajouter dans la procédure une vérification de cette adresse électronique pour chaque utilisateur.

• La liste de révocation qui contient la liste des certificats qui ont été révoquées, suite à une perte de clé privée ou à une divulgation de cette clé ou à un changement de statut inattendu du propriétaire du certificat (changement d'organisme, de laboratoire, ...) n'est pas simple à gérer. Il faut la recharger “manuellement” et régulièrement dans les navigateurs.

• Plusieurs utilisateurs, pourtant administrateurs informatiques avertis ont “perdu” leur clé privée (oubli du mot de passe pour l'utiliser, crash de leur système qui efface cette information, ...) . Il faut impérativement une sensibilisation pour que la sauvegarde de cette clé devienne un réflexe.

Dans l'utilisation de ces certificats, il est apparu que les outils Netscape et Internet Explorer sont loin d'être parfaits. Netscape par exemple affiche une icone “Invalid Signature” quand la liste de révocation de l'autorité de certification qui a délivré le certificat est plus récente que la signature. Ainsi lorsque vous rechargez une liste de révocation, certains anciens messages tout à fait corrects apparaissent alors avec une signature invalide. Il est difficile de faire comprendre ce bogue à des utilisateurs non informaticiens..

Pour prendre un exemple d'utilisation de ces certificats CNRS-Test, ils ont été délivrés à certains coordinateurs et correspondants sécurité CNRS [Organisation sécurité CNRS]. Dans cette communauté ils ont servi à signer les avis des CERTs rediffusés par l'UREC (fonction d'authentification de l'émetteur d'un message électronique et d'intégrité), signer et chiffrer certains échanges confidentiels concernant des problèmes de sécurité (fonction de confidentialité d'un message électronique), accéder à des pages Web réservées à cette population (fonction d'Intranet en lecture), préparer un cours de sécurité [SIARS] avec une douzaine d'auteurs de plusieurs régions (fonction d'Intranet en lecture et écriture). Tout ceci a montré qu'une fois les certificats délivrés, ils peuvent être utilisés pour de nombreuses applications très rapidement.

Ces tests et la phase pilote le confirme, ont aussi montré que actuellement l'utilisation la plus intéressante et la plus facile des certificats n'est pas la messagerie comme on pourrait le penser, mais le contrôle d'accès sur les pages Web ou pour accéder a des applications. Concernant la messagerie, la fonction prioritaire demandée est la signature, loin devant le chiffrement.

A noter qu'en parallèle a été menée une autre expérimentation pilotée par Roland Dirlewanger [Dirlewanger] avec les laboratoires de la délégation de Bordeaux, pour des applications plus de gestion et avec une autre procédure pour délivrer des certificats : l'utilisation d'une disquette contenant le certificat et la clé privée donnée en main propre à chaque utilisateur. Ceci a permis ainsi de comparer les 2 types de procédures. La conclusion a été que la diffusion par disquette était très lourde et ne supporterait pas le changement d'échelle.

En résumé CNRS-Test a été une très bonne démystification des IGC et nous a permis d'évaluer les possibilités des certificats ainsi que les briques nécessaires pour une IGC. Cela nous a aussi confirmé que dans ce domaine il faut être prudent et avancer pas à pas.
Mais les services rendus par les certificats étaient déjà très utiles et les applications avaient été simples à mettre en place. Il a été décidé de continuer dans cette voie.

## 3. L'IGC CNRS

Suite aux premiers résultats de la plate-forme CNRS-Test, en juillet 2000 le CNRS a décidé de créer une IGC et d'en confier la mise en oeuvre à l'UREC [BO CNRS]. Un comité de pilotage et un comité technique ont été créés pour définir la politique de certification et les procédures nécessaires. Ce travail se poursuit toujours et le document "Politique de certification et procédures de l'autorité de certification CNRS" [CNRS-PC] est tenu à jour pour suivre les évolutions. Ce travail se fait en respectant les recommandations ministérielles et en contact étroit avec la DCSSI [DCSSI].
Lorsque l'on monte une IGC il faut obligatoirement définir à qui l'on va distribuer des certificats, pour quel usage, de quelle manière, avec quelle architecture et quels produits d'IGC, ainsi que le contenu des certificats.

### *3.1 Des certificats pour quels usages, avec quels produits ?*

L'objectif peut paraître ambitieux mais on désire utiliser des certificats CNRS pour tous les usages possibles, c'est à dire avec toutes les applications où ces éléments peuvent être utiles, pour couvrir par exemple tous les besoins cités dans le paragraphe 1 mais aussi les nouvelles applications qui vont apparaître. Donc des certificats multi usages. On ne veut pas non plus se limiter aux échanges intra CNRS mais pouvoir les utiliser à long terme dans les communications scientifiques, administratives, commerciales, ... avec tous les autres partenaires. Evidemment cela prendra du temps mais on peut dès à présent mettre en place ce qu'il faut pour que ce que les certificats délivrés puissent dans quelques années à venir avoir ce large spectre d'utilisation.

Plus concrètement, avec quels logiciels clients utilisateurs aujourd'hui ? De part son organisation et son ouverture, une des contraintes du CNRS dans ce domaine et plus généralement pour toute l'informatique dans les laboratoires est d'utiliser les produits courants, de navigation et de messagerie entre autres, ainsi que les standards. Il serait déraisonnable d'opter pour des solutions propriétaires et des produits spécifiques de navigation et de messagerie. Mais une entreprise ou une administration très centralisée peut avoir un objectif inverse, ce qui peut être totalement justifié et judicieux. Nous avons donc choisi de supporter en priorité les versions récentes de Netscape et Internet Explorer comme outils utilisateurs de messagerie et de navigation.

Nous avons un grand parc d'utilisateurs d'Eudora et Eudora n'utilise pas actuellement les certificats. Il y a donc un problème. Il existe des logiciels (des sociétés Baltimore et MSI par exemple) qui permettent d'"ajouter" cette fonction dans Eudora, mais ils sont incomplets. De plus, le logiciel Eudora ne semble pas beaucoup progresser et donc il faudrait faire migrer ces utilisateurs vers un autre outil de messagerie. Mais lequel ? Netscape est un bon produit, qui a l'avantage de tourner aussi sous Unix, mais lui aussi semble un peu en panne de développement. Mais le choix d'un outil de messagerie sort du sujet de cet article. Nous pensons donc tester plus à fond les logiciels Baltimore et MSI pour éventuellement les préconiser durant une période transitoire aux utilisateurs qui veulent continuer avec Eudora. D'un autre côté, pour différentes raisons, la messagerie ne sera certainement pas la première application des certificats, donc le problème d'Eudora n'est pas bloquant.

Concertant un choix d'utilisation en terme de service de sécurité, l'IGC CNRS délivrera des certificats pour la signature (authentification et intégrité) et des certificats pour le chiffrement (confidentialité). Pour suivre les recommandations du DCSSI, pour le premier type, l'utilisateur sera le seul à connaître sa clé privée, pour le second un séquestre des clés privées sera assuré. Dans la phase pilote et jusqu'à présent, uniquement des ertificats de signature ont été délivrés. Ils correspondent au besoin prioritaire et le séquestre des clés privées est un sujet délicat. Il doit être assuré avec beaucoup de précautions, à la fois techniques, mais aussi dministratives et juridiques, peut-être par un tiers.

### *3.2 Des certificats pour qui ?*

Il a été décidé de pouvoir délivrer des certificats à toute personne qui travaille dans un laboratoire ou service CNRS, agent CNRS ou non, permanent ou non, et de l'étendre à toute personne qui a besoin d'un certificat dans le cadre de collaborations avec le CNRS. Ceci n'est pas une volonté hégémonique, mais est une décision pragmatique dans le sens où il faut que les certificats puissent être utilisés dans nos applications courantes par les laboratoires. Or dans les mois à venir nous allons être les seuls à pouvoir délivrer rapidement des certificats dans les laboratoires. Et la grande majorité des laboratoires CNRS n'ont pas que du personnel CNRS, le directeur est même souvent un universitaire. Dans une telle configuration, il serait complètement inutile d'être plus restrictif actuellement, par exemple en ayant uniquement des certificats pour les agents CNRS.





Outre les certificats de personnes, il est délivré aussi des certificats pour des services (serveurs Web par exemple) et pour la signature de code (applets JAVA par exemple). Il nous est déjà parvenu plusieurs demandes pour ce dernier type de certificat, alors que nous pensions que ce n'était pas une priorité.

### *3.3 Les logiciels*

La plate-forme CNRS-Test a montré que le nombre de lignes de code d'un produit d'IGC est relativement faible et qu'en prenant des éléments de OpenSSL ou en s'en inspirant, on pouvait assez facilement développer ce type de logiciel. Les tests ont aussi confirmé que le CNRS est une organisation complexe est qu'il n'est pas organisé comme une entreprise classique, le schéma de l'IGC décrit plus loin en témoigne. Dernier élément, nous avons fait rapidement le tour des produits commerciaux IGC mi 2000. Ceux-ci étaient très cher, très rigides et certains imposaient des clients spécifiques sur les postes utilisateurs.
Nous avons donc décidé de développer notre propre code IGC. Ce développement fait par Claude Gross [cg] et Philippe Leca [pl] a débuté en septembre 2000 et une première version a été mise en oeuvre en mai 2001.

### *3.4 L'architecture de l'IGC*

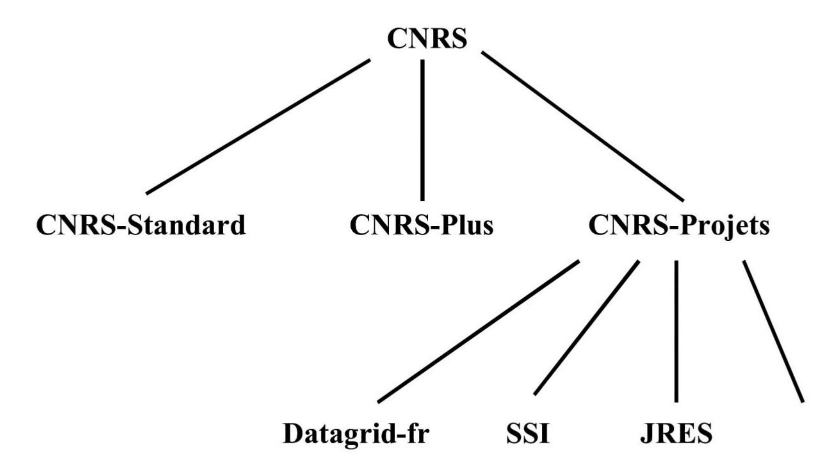
Le certificat de l'autorité de certification CNRS est signé par elle-même (autorité auto-signée). Actuellement, il n'y a pas d'autorité gouvernementale française qui puisse signer des certificats d'autorités de certification, donc nous n'avons pas eu d'autre choix, il était hors de question d'utiliser une autorité commerciale. Lorsqu'une telle autorité au niveau du premier ministre ou du ministère pourra effectuer cette signature, le DCSSI devrait en monter une, le CNRS sera candidat pour que le certificat de son autorité de certification soit signé par cette autorité.

Vu la structure de l'organisme et les besoins, nous avons créé une arborescence d'autorités de certification. Une autorité racine CNRS a trois autorités filles :

• CNRS-Standard, signée par l'autorité CNRS. Elle délivre des certificats utilisateurs, de services et de codes pour des utilisations courantes.

• CNRS-Plus, signée par l'autorité CNRS. Elle délivre des certificats utilisateurs pour les actes importants et pour des personnes ayant une fonction de direction. Il se peut que dans un futur proche, les certificats délivrés par cette autorité soit sur un support particulier jugé plus sécurisé qu'un simple fichier, une carte à puce par exemple.

• CNRS-Projets, signée par l'autorité CNRS dont le but est de pouvoir délivrer des certificats (utilisateurs, services ou codes) pour des projets auxquels participent plusieurs laboratoires, des organismes non CNRS, avec des durées de vie limitées, ... Sous cette autorité on créera autant de sous autorités (cf chapitre Sites pilotes) que de projet. Chaque sous-autorité sera signée par l'autorité CNRS-Projets.




L'autorité de certification CNRS-Test continue d'exister pour des tests ou pour des utilisations qui ne rentrent pas dans ce schéma actuellement, mais avec les nouveaux logiciels IGC et les nouvelles procédures décrites ci-après.

Les autorités d'enregistrement sont les personnes qui vérifient les informations fournies par les utilisateurs et qui donnent leur feu vert à l'autorité de certification pour délivrer ou non un certificat à ces utilisateurs.
Chaque autorité d'enregistrement de l'IGC CNRS dispose d'un certificat CNRS-Plus, pour ses actions liées à l'IGC.

Pour les certificats CNRS-Standard, dans chaque laboratoire, l'autorité d'enregistrement est le directeur du laboratoire ou son représentant (désigné par le directeur, l'équivalent d'une délégation de signature). Cette autorité d'enregistrement peut accepter les demandes de certificats CNRS-Standard des personnes du laboratoire (permanents ou non). Une même personne peut être autorité d'enregistrement pour plusieurs laboratoires (fédération par exemple ou regroupement de petites unités ou prise en charge de cette fonction au niveau de la délégation). Cette vérification et cette décision est donc totalement décentralisée, placée au niveau du directeur du laboratoire, seule personne qui peut connaître tout son personnel et donc faire les vérifications nécessaires. Il peut par exemple savoir combien de temps va rester un stagiaire et délivrer un certificat avec une date de validité limitée à la présence du stagiaire.

Pour les certificats CNRS-Plus, les autorités d'enregistrement seront des personnes avec une haute responsabilité dans le CNRS comme les Délégués par exemple. Actuellement les certificats CNRS-Plus n'ont été délivrés qu'à des autorités d'enregistrement de CNRS-Standard et de CNRS-Projets et l'autorité d'enregistrement a été l'UREC. Ceci ne devrait pas perdurer.

Pour les certificats des sous-autorités sous CNRS-Projets, l'autorité d'enregistrement est le responsable du projet ou son représentant.

Pour CNRS-Test l'autorité d'enregistrement est actuellement l'UREC.

Les certificats sont au format X509V3 [X509V3]. Ils utilisent un algorithme de chiffrement RSA avec des clés de 1024 bits par défaut (512 ou 2048 éventuellement).

Les certificats de personnes et de services sont délivrés avec une durée de vie par défaut de un an. Ce peut-être moins (personnel temporaire par exemple). C'est l'autorité d'enregistrement qui décide.

A la fois parce que ce sont des documents publics et parce qu'il faut que les informations contenues dans le certificat soient assez stables dans le temps, les certificats CNRS contiennent peu d'informations. Les certificats de personnes CNRS-Standard et CNRS-Plus contiennent le prénom, le nom, l'adresse électronique, le code de l'unité (si la personne travaille dans une unité CNRS), l'organisme (CNRS ou EXTERNE) et le pays. Pour les sous-autorités de CNRS-Projets, cela dépend des projets. Pour les services, il contient le nom de la machine sous forme de domaines et l'adresse électronique de l'administrateur.

Les listes de révocations pour chaque autorité sont publiées chaque nuit avec une durée de validité de un mois.

Un annuaire LDAP tenu à jour, en accès public permet de récupérer les certificats des personnes et des services.

### *3.5 Les procédures*

On peut rappeler que chaque laboratoire ou projet a une autorité d'enregistrement. Cette autorité possède un certificat CNRS-Plus.
Pour obtenir un certificat de personne CNRS-Standard ou d'une sous autorité de CNRS-Projets destiné à la signature (sans séquestre de clé privée) la procédure est la suivante.

- L'utilisateur avec Netscape ou Internet Explorer accède à un formulaire électronique en ligne. Ce formulaire lui demande son nom, prénom, adresse électronique, … toutes les données qui vont figurer dans son certificat. Le formulaire rempli, la création d'un couple de clés privée-publique est provoquée sur le poste utilisateur. Le poste utilisateur conserve la clé privée, la clé publique est « récupérée » par le serveur.
- Un message électronique, pour confirmation et vérification d'adresse électronique, est envoyé à l'utilisateur, qui l'acquitte.
- Le formulaire (avec la clé publique de l'utilisateur) est stocké dans un spool. L'autorité d'enregistrement est avertie par messagerie électronique qu'une demande de certificat est arrivée.
- L'autorité d'enregistrement accède à cette demande avec son navigateur et son certificat CNRS-Plus. Elle vérifie les informations contenues dans la demande, contacte le demandeur pour vérifier qu'il a bien fait cette demande (et possède la clé privée associée). Si tout est bon, elle acquitte la demande. Celle-ci est transmise à l'autorité de certification.
- L'autorité de certification (un automate) crée le certificat , le dépose sur un serveur Web et dans l'annuaire LDAP des certificats CNRS, puis envoie un message électronique à l'utilisateur.
- L'utilisateur récupère son certificat sur le serveur Web.

Les différentes demandes et toutes les opérations sont archivées.





## 4 Les sites pilotes

Depuis mai 2001, nous avons mis en place des sites pilotes qui sont pour les certificats CNRS-Standard : le laboratoire LAAS à Toulouse, le LMCP de Jussieu, les laboratoires de l'IMAG à Grenoble, six laboratoires de la délégation de Toulouse, environ 45 laboratoires de la délégation de Bordeaux, la DSI.

Sous CNRS-Projets nous avons créé les autorités SSI pour les coordinateurs et correspondants sécurité CNRS, Datagrid-fr pour le projet Datagrid, JRES pour certains membres du comité de programme, d'organisation et certains intervenants. Début septembre deux demandes sont en cours pour créer un projet pour le groupe technique de RAP (Réseau Académique Parisien) et pour les MSH (Maisons des Sciences de l'Homme).

Au total il y a presque 60 autorités d'enregistrement.
Début septembre nous n'avons pas fait de bilan d'utilisation avec ces différents sites mais il y a convergence vers les contrôles d'accès liés au Web. Pour le projet Datagrid les certificats sont vitaux; En effet, il est obligatoire que chaque utilisateur et chaque ressource dispose d'un certificat pour utiliser la grille avec le logiciel utilisé Globus.

L'UREC administre les machines sur lesquelles tournent les logiciels IGC. Début septembre ont été délivrés et sont toujours valides 589 certificats : 225 certificats CNRS-Test, 59 certificats CNRS-Plus, 163 CNRS-Standard, 76 Datagrid-fr, 59 SSI, 7 JRES.

La page Web [Web IGC CNRS] permet d'accéder à tous les formulaires pour demander ou rechercher des certificats dans l'IGC CNRS.

Un premier constat est que sans des procédures en ligne et des autorités d'enregistrements décentralisées, nous n'aurions pas pu délivrer autant de certificats avec néanmoins des règles de vérification strictes.

## 5 Les choix avant le déploiement

Avant de déployer les certificats pour l'ensemble du CNRS, il est nécessaire de faire différents choix pour que le service soit fiable, stable et rende les services attendus. Voici les questions qui se posent, certaines laissées un peu sans réponse, car elles sont en cours de réflexion.

Il faut bien prendre conscience du rôle très important que joue une IGC et de la fiabilité qu'elle doit avoir. On pense souvent que le seul problème critique est la clé privée de l'autorité de certification qui doit être ultra secrète. Ce n'est pas le seul. En effet, pour que les certificats soient largement utilisés, en particulier dans toutes les applications de gestion qui peuvent être critiques (comptabilité, paye par exemple), il faut que ce logiciel soit très stable. Il est exact qu'il n'y a pas besoin que l'IGC soit opérationnelle pour utiliser les certificats délivrés par elle. Néanmoins il faut qu'elle perdure dans le temps et puisse délivrer des certificats rapidement. Imaginez un agent comptable dont le certificat arrive à expiration, avec une IGC "en panne", qui ne puisse pas le renouveler !

Il faut dans un premier temps que le logiciel soit maintenu. Actuellement le logiciel IGC CNRS est un logiciel développé par l'UREC. L'UREC n'est ni une société de développement, ni de maintenance logiciel et n'a pas vocation à le devenir. Il faut donc peut-être envisager de sous-traiter la maintenance de ce développement à un autre service du CNRS ou à une société commerciale. Par contre, il faut garder la possibilité de faire évoluer le logiciel. L'utilisation des certificats n'est pas figée, de nouvelles applications vont arriver, de nouvelles communautés d'utilisateurs, il faudra que le logiciel s'adapte. Un exemple s'est déjà produit. Le projet Datagrid a déjà demandé des spécificités dans la structure des certificats, il est évident que d'autres projets vont demander d'autres spécificités et qu'il faut que le logiciel puisse y répondre.

Les machines qui hébergent l'IGC et en particulier les clés privées des autorités de certification doivent être dans des lieux très protégés (des blockhaus ?). Elles sont actuellement dans des lieux à salles à accès très contrôlé mais pas avec un niveau de sécurité suffisant. Il faudra les faire héberger dans des centres de services CNRS adaptés ou par une société commerciale. En parallèle se pose la question de la déconnexion complète du réseau des machines qui génèrent les certificats. Nous pensons que l'on peut très bien protéger une machine même si il existe un lien avec l'extérieur, avec des filtres, des garde-barrières, ... Mais pour rassurer les personnes non spécialiste en réseau, il se peut qu'il faille que l'on déconnecte complètement ces machines et que la création de certificats nécessite une intervention humaine (manipulation de disquette ou CD par exemple). Il faudra alors prévoir des opérateurs habilités, avec une astreinte, ...

L'utilisation de la carte à puce semble pouvoir apporter plus de sécurité dans la protection de la clé privée et dans l'utilisation des certificats sur des postes non personnels. Je ne répéterai pas le discours sur ce sujet (c'est un objet que l'utilisateur ne prêtera pas facilement ...). Le problème technique est qu'actuellement il n'y a pas de standard de carte à puce, en tous cas pour les certificats et les fonctions de cryptographie. Il est donc illusoire de penser que chaque utilisateur peut avoir une carte à puce et l'utiliser sur n'importe quel poste. Il faut choisir un modèle de carte et installer les lecteurs, pilotes et interfaces adaptés. Il faut aussi définir les fonctionnalités de cette carte et ce qu'elle contient. En effet, pour qu'elle apporte une bonne sécurité, il faut que la clé privée de l'utilisateur ne quitte jamais la carte, qu'elle ne soit pas copiée en mémoire sur l'ordinateur

par exemple. Il faut donc les fonctions de chiffrement, déchiffrement, signature, ... s'exécutent sur la carte. Ce n'est pas le cas de toutes les cartes. Un autre aspect à prendre garde est qu'il faut être prêt à redonner une carte à chaque utilisateur en cas de perte ou de détérioration, donc il faut pouvoir en régénérer très rapidement. Les cartes à puce seront certainement utilisées au CNRS mais dans des communautés limitées, peut-être avec des postes particuliers.

Il faudra aussi distribuer des certificats pour le chiffrement et donc assurer un séquestre des clés privées. Il serait peut-être souhaitable que ce séquestre soit assuré par un tiers, espèce de notaire.

Un autre point que l'on a à résoudre c'est la désignation des autorités d'enregistrement qui délivreront des certificats CNRS-Plus, dans un premier temps aux autorités d'enregistrement dans les laboratoires. Il faut qu'elles connaissent bien les laboratoires et leur direction. Une solution serait que ces autorités soient au niveau de chaque délégation du CNRS.

L'utilisation d'un certificat et de tout ce qui va avec (clés, liste de révocation, ...) n'est pas simple. Il faut donc impérativement prévoir une assistance pour les utilisateurs. Les problèmes soulevés seront très souvent liés aux applications, comme les logiciels de gestion, qui vont utiliser les certificats. Il serait peut-être bénéfique de rattacher cette aide à celle apportée au niveau des délégation au support de XlLab par exemple.

Comment développer les applications qui utiliseront les certificats ? Ce n'est pas le problème de l'IGC. Le but de l'IGC est de délivrer des certificats avec des procédures de vérification strictes, certificats avec un format utilisable par les applications. Ce sont les deux demandes que doit couvrir l'IGC. Si elles sont bien remplies les applications fleuriront d'elles-mêmes. C'est un autre travail. Ca paraît même plus rationnel et plus sécurisé de séparer ces activités. De plus, il ne faut vouloir trop en faire, le sujet est déjà assez complexe.

Autre question qui va rapidement se poser : comment communiquer avec les autres organismes qui ont leur propre IGC ? C'est aussi un vaste débat pour les personnes qui installent des IGC. Si le DCSSI signe les certificats des autorités de certification des ministères, une possibilité sera de faire confiance à cette racine française et de fait à toutes les autorités "signées" par le DCSSI. Si ce n'est pas le cas ou pour les autres autorités, il faudra avoir des accords avec chacune et se reconnaître mutuellement. Pour ce faire le document qui décrit la politique et les procédures de certification de chaque IGC servira pour déterminer si on peut faire confiance à l'IGC ou pas. Dans le projet européen Datagrid, il y a plusieurs autorités de certification, une par pays. Pour se faire reconnaître par les autres, chacune à décrit sa politique et ses procédures dans un document dont la structure est conforme à un RFC qui indique un canevas précis pour décrire ces éléments [RFC2527]. L'IGC CNRS a ainsi produit le document "Certificate Policy and Certificate Practice Statement CNRS/CNRS-Projets/Datagrid-fr" [CNRS.cps].

En fait, le principal problème actuellement et qui va certainement freiner le déploiement, est beaucoup plus concret. C'est d'un côté la méconnaissance du sujet, des utilisateurs mais aussi des administrateurs, et de l'autre la mauvaise ergonomie et les bogues des outils. En effet, outre le problème de Eudora, que ce soit Netscape ou Internet Explorer, l'installation des certificats et les options à choisir sont très difficiles à comprendre pour des utilisateurs non familiers avec le sujet car mal présentés. Ensuite l'utilisation est simple si l'utilisateur n'a qu'un seul certificat et une seule autorité de certification. Dans le cas contraire cela redevient compliqué, il y a aussi parfois des bogues. Or nous sommes désarmés pour faire évoluer ces outils, on ne peut qu'espérer qu'ils s'amélioreront ou qu'il y en aura d'autres. Si les certificats se répandent, ce sera le cas.

## 6 Quelques mises au point

Les certificats peuvent rendre de très nombreux services. Néanmoins, on peut émettre deux réserves.

La première concerne la confiance. En effet, tout IGC nécessite des procédures strictes et sérieuses pour assurer les garanties qui sont affichées. Mais s'il s'avère que ces procédures ne sont pas fiables, il y aura des malversations, des faux certificats, … Si ces incidents sont trop nombreux, alors plus personne ne fera confiance aux certificats et ceux-ci n'auront plus aucune valeur. Ce sera la mort des certificats. Ceci est d'autant plus préoccupant que tout ce secteur est totalement libéralisé, laissé aux entreprises privées. Or, celles-ci peuvent avoir tendance à négliger les procédures (coûteuses) pour un profit à court terme. Des certifications et des vérifications par des organismes gouvernementaux sont nécessaires et elles commencent à apparaître mais le contrôle sera délicat s'il ne veut pas être trop lourd.

La seconde est l'aspect sécurité informatique, au sens classique d'aujourd'hui. Dans ce domaine, les certificats ne vont pas résoudre tous les problèmes. En étant provocateur, on peut même se demander, s'ils amélioreront réellement la sécurité actuelle. Ce n'est pas une conséquence automatique. Les certificats sont de très bons outils mais ce ne sont que des outils. Outre le problème des IGC mal conçues et des certificats mal gérés, il reste le problème de l'utilisation. Car mal protégée par les utilisateurs, la clé secrète (et le certificat associé) ne sera pas plus fiable qu'un mot de passe qui circule en clair sur le réseau ou qui est noté sous le clavier. Mais finalement, ceci n'est pas le problème des certificats et des IGC. C'est un problème classique de sécurité : la sensibilisation des utilisateurs. Elle devra être faite dès les premières utilisations de certificats.
Les certificats ne résoudront pas non plus les problèmes d'intrusions ou de rupture de service par l'utilisation





de failles de sécurité dans les logiciels, la prolifération de virus en tous genres, … Il faudra toujours des architectures sécurisées, des contrôles d'accès dans ces architectures, des anti-virus, …

On peut prévoir aussi que les certificats comme tout nouveau service informatique apporteront leurs propres problèmes de sécurité.

Mais ne noircissons pas trop le futur. Si l'introduction des certificats dans un organisme ou une entreprise est correctement réalisée, avec professionnalisme et méthode, le gain en terme de sécurité et de nouvelles facilités de contrôles devrait être très important.

On peut penser aussi que plus que l'amélioration de l'existant en terme de sécurité, l'intérêt des certificats réside dans les nouveaux services qu'il sera beaucoup plus facile de mettre en place, en particulier dans des structures très éclatées géographiquement comme le CNRS.

***Références***


[BO CNRS]
Décision de création d'une autorité de certification CNRS
*http://www.urec.cnrs.fr/securite/articles/decision_creation_AC_cnrs*

[Certificats]
Article "Certificats (électroniques) : Pourquoi ? Comment ?" JL Archimbaud
*http://www.urec.cnrs.fr/securite/articles/certificats.kezako.pdf*

[cg]
*http://www.urec.cnrs.fr/urec/annuaires/gross.html*

[CNRS.cps]
Certificate Policy and Certificate Practice Statement CNRS/CNRS-Projets/Datagrid-fr
*http://www.urec.cnrs.fr/igc/Doc/Datagrid-fr.policy.pdf*

[CNRS-PC]
Politique de certification et procédures de l'autorité de certification CNRS
*http://www.urec.cnrs.fr/securite/articles/PC.CNRS.pdf*

[CNRS-Test]
Article "Autorité de certification CNRS-Test gérée par l'UREC" JL Archimbaud
*http://www.urec.cnrs.fr/securite/articles/CA.CNRS-Test.pdf*

[Datagrid]
Projet Datagrid
*http://web.datagrid.cnr.it/*

[DCSSI]
Direction Centrale de la Sécurité des Systèmes d'Information
*http://www.ssi.gouv.fr/*

[Décret signature électronique]
Décret no 2001-272 du 30 mars 2001 relatif à la signature électronique
*http://www.legifrance.gouv.fr/citoyen/jorf_nor.ow?numjo=JUSC0120141D*

[Dirlewanger]
Roland Dirlewanger, responsable du STI de la délégation de Bordeaux
*http://www.dr15.cnrs.fr/Delegation/STI/*

[HTTPS]
RFC2817 : Upgrading to TLS Within HTTP/1.1
*http://www.pasteur.fr/cgi-bin/mfs/01/28xx/2817*

[IGC]
Article "Infrastructures de Gestion de Clés" N. Dausque
*http://www.urec.cnrs.fr/securite/articles/IGC.pdf*
FAQ IGC du DCSSI
*http://www.scssi.gouv.fr/fr/faq/faq_igc.html*

[IPSec]
Ensemble de documents sur IPSec
*http://www.hsc.fr/ressources/veille/ipsec/index.html.fr*

[jla]
*http://www.urec.cnrs.fr/jla*

[OpenCA]
Serveur du projet OpenCA
*http://www.openca.org/*

[OpenSSL]
Serveur du projet OpenSSL
*http://www.openssl.org/*

[Organisation sécurité CNRS]
*http://www.urec.cnrs.fr/securite/CNRS/organisation.html*
[pl]
*http://www.urec.cnrs.fr/urec/annuaires/leca.html*
[RFC2527]
Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
*http://www.pasteur.fr/infosci/RFC/25xx/2527*
[RSA]
*http://rsasecurity.com/rsalabs/*
[S/MIME]
S/MIME Working Group
*http://www.imc.org/ietf-smime/*
[SSH]
Page d'accueil pour la communauté des utilisateurs de SSH
*http://www.ssh.org/*
[SSL]
Introduction to SSL
*http://developer.netscape.com/docs/manuals/security/sslin/index*
[Web IGC CNRS]
*http://www.urec.cnrs.fr/igc/Certifs_CNRS.html*
[X509V3]
RFC2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile
*http://www.pasteur.fr/cgi-bin/mfs/01/24xx/2459*



